ABSTRACT OF THE DISCLOSURE

A technique to bootstrap a secure communications channel between devices via a cryptographic key. A key is generated by a first device and a copy of the key is sent to a second device via a short range wireless communication channel so as to provide each device with a shared key. In one embodiment, the short range channel comprises a transponder/transponder reader pair in which the transponder is placed in proximity to the transponder reader to enable communication between the devices. Upon receipt of the shared key, symmetric authenticated key agreement algorithms, one for each device, are executed to cooperatively generate a cryptographic key that is used to provide for a secure communication channel using an encrypted communication protocol based on the cryptographic key. The invention removes the necessity of entering userIDs, passwords, and the like at devices to enable the creation of shared cryptographic keys.